University of
South Australia

School of Information Technology & Mathematical Sciences
Division of Information Technology, Engineering and the Environment

An evidence-based cloud incident handling framework

By

Nurul Hidayah Ab Rahman

Principal Supervisor: Associate Professor Kim-Kwang Raymond Choo
Co-Supervisor: Professor Andy Koronios

A thesis submitted for the degree of

Doctor of Philosophy

June 2016

Table of contents

List of figures

List of tables

Abbreviations

API	Application Programming Interface
Apps	Applications
CPCS	Cyber-Physical Cloud System
CPS	Cyber-Physical System
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
CSU	Cloud Service User
DFR	Digital Forensic Readiness
EFA	Exploratory Factor Analysis
ENISA	European Network and Information Security Agency
FBD	Forensic by Design
FTP	File Transfer Protocol
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IHSA	Incident Handling Strategy Adoption
IPS	Intrusion Prevention System
IS	Information Security
ISO	International Organization for Standardization
KMO	Kaise-Mayer-Olkin
NIST	National Institute of Standards and Technology
OBU	On Board Unit
OSSIM	Open Source Security Information and Event Management
PaaS	Platform as a Service

PMT	Protection Motivation Theory
PSEV	Perceived Severity
PVUL	Perceived Vulnerability
RAT	Routine Activity Theory
RCO	Response Cost
REF	Response Efficacy
RSU	Road Side Unit
SA	Situational Awareness
SaaS	Software as a Service
SEF	Self-efficacy
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
StaaS	Storage as a Service
VANET	Vehicular Ad Hoc Network
VM	Virtual Machine
WebDAV	Web-based Distributed Authoring and Versioning

Abstract

Cloud computing is increasingly adopted by both individual and organisational users; thus, ensuring the security and privacy of data stored in the cloud is a crucial requirement in an organisation's business continuity and risk assessment strategies. An incident handling strategy is key to mitigating risks to the confidentiality, integrity and availability of information assets, particularly those outsourced to the cloud located in one or more different countries. Thus, organisational cloud users may face challenges or be limited in their capability to handle security incidents (e.g. security breaches) on their sites since the infrastructure on which the data resides belongs to the cloud providers.

Surveys were conducted with industry practitioners to identify: (1) the implications of emerging technologies and its information security threats on the incident handling practices, and (2) the factors influencing incident handling adoption for organisational cloud users. The results indicated that the current landscape of information security threats have impacted on their security strategic planning, resulting in practitioners being more proactive, requiring better tactical tools, and cultivating a culture of information security. The factors identified as having a significant influence on the adoption were determined using an integration of Situational Awareness and Protection Motivation Theory. Users are more likely to adopt if they are aware of cloud security and privacy related risks, confident in their capability, understand the benefits, and understand the impact due to an ineffective strategy.

The cloud incident handing framework presented in this thesis draws upon principles and practices from both incident handling and digital forensics. The integration of digital forensic principles and practices facilitates the collection of digital evidence, reconstructing of events and establish facts of who, what, when, where, how, and why an incident took place. The framework consists of six phases, namely: Preparation (integrated with forensic readiness principles); Identification; Assessment (integrated with forensic collection and analysis practices); Action and Monitoring; Recovery; and Evaluation (integrated with forensic presentation practices). A feasibility study was conducted that simulates private cloud storage (i.e. ownCloud) in a virtual environment. A security information and event management tool was used to demonstrate that each phase is feasible with significant evidence artefacts can be collected.

This framework was also validated using two case studies: mobile cloud storage (Google Drive, Dropbox, and OneDrive) and mobile communication (Viber, Telegram, Skype, WhatsApp and Messenger) applications. Both studies simulated typical user activities on the studied applications on the Android platform. Mobile forensics and network tools were deployed for the collection and analysis of evidence artefacts. The first case study simulated uploads, share, read and download files. The artefacts were then analysed based on the activities. The second case study was setting up the scenario of terrorists' use of mobile communication applications by simulating chat conversation, adds contacts, and shared media files activities. The artefacts were classified into accounts, contacts, chat logs, shared media files, and location data to facilitate terrorism investigations.

This research has shown that the framework supports organisational users in both the incident handling and forensic investigations, as well as informing the design of security strategies for organisations.

Acknowledgements

I am very thankful and grateful to have crossed paths with many wonderful people who have helped me in many ways in my pursuit of a PhD at the School of Information Technology and Mathematical Sciences, University of South Australia.

Foremost, I would like to express my gratitude to my principal supervisor, Associate Professor Kim-Kwang Raymond Choo, and co-supervisor, Professor Andy Koronios, for their supervision and advice from the very early stages of this study through to the completion of this thesis. Their guidance and support have been of great value.

Special thanks go to my co-authors, family, friends, Research Education Advisers from the Teaching Innovation Unit, and all the Information Assurance Research Lab members, who have helped and supported me over these years.

This study was financed with the aid of scholarships from the Ministry of Education in Malaysia and the Universiti Tun Hussein Onn Malaysia, and I would like to thank them for those scholarships.

1 Introduction

1.1 Research background

The pervasive interconnectivity of systems (e.g. cloud computing and Internet of Things) used in our Internet-connected society can potentially be, and have been, exploited by actors with malicious intents, ranging from cyber criminals acting alone to organised groups of financially-, criminally- and issue/ideologically-motivated crime groups to state-sponsored actors (Choo 2011). It is not surprising that information security incidents are increasing in both number and the level of sophistication. For example, Symantec Corporation (2016) reported that more than 430 million new types of malware were discovered, the number of spear-phishing attacks targeting employees increased 55 percent, and crypto-style ransomware grew 35 percent in the fiscal year 2015. Of note, the report highlighted that security incidents moved to new targets such as smart phones, Mac and Linux systems, and cloud computing environments.

The increasing trend of organisations moving sensitive data to cloud infrastructure has resulted in an urgent need to ensure that security and privacy safeguards are in place, as cloud services are potential criminal targets due to the amount of sensitive organisational data stored in the cloud. As surveyed by the Cloud Security Alliance (CSA) (2016), industry experts identified 12 critical issues to cloud security with data breaches, poor credential management, and insecure application programming interfaces (APIs) being the top three. A proactive incident handling strategy is one key approach to mitigating risks to the confidentiality, integrity and availability (CIA) of assets, as well as minimising loss (e.g. financial, reputational and legal) in a dynamic cloud environment. Existing information security incident handling strategies, however, may not be adequate as cloud data would generally be virtualised, geographically distributed and ephemeral, presenting both technical and jurisdictional challenges. This is consistent with CSA's report entitled 'Security Guidance for Critical Areas of Focus in

Cloud Computing', which highlights three critical focus areas, namely Incident Response, Notification and Remediation (Cloud Security Alliance 2011).

In investigating and responding to computer security incidents, digital forensics can play a crucial role (Cichonski et al. 2012; Freiling & Schwittay 2007; Gurkok 2013). Forensic tools and techniques are not only useful for criminal prosecution in a court of law, but also for various other tasks within an organisation, such as event reconstruction (i.e. who, what, when, where, how, and why an incident took place), data or system recovery, and system operation troubleshooting (Kent et al. 2006). Similarly, incident handling is not only for responding to incidents, but more importantly, identifying the root causes to prevent similar breaches from reoccurring. Therefore, incorporating forensically sound practices in an incident handling strategy would support cloud service users (CSUs) to be better prepared, more proactive, and forensically ready when analysing an incident.

In this thesis, an evidence-based cloud incident handling framework that integrates digital forensic practices into incident handling strategies is presented, which is designed to allow organisational cloud service users to respond to and investigate incidents more effectively.

1.2 Problem statement

A successful security incident occurrence or breach can cause direct (e.g. theft of intellectual property or customer data) and/or indirect losses (e.g. reputational or legal) to organisation assets, and can have significant financial implications. Cloud service users (CSUs) and cloud service providers (CSPs) are increasingly at risk of cyber incidents, both intentional and unintentional, and by both individuals and organised groups (Choo 2010; Hooper, Martini & Choo 2013; Martini & Choo 2012).

Despite the associated security risks, organisations benefit from migrating to cloud-based services such as cost-effectiveness, scalability, and flexibility. Hence, engaging a strategy to handle security incidents is the key to striking a balance between cost-effectiveness and security controls. Both CSPs and CSUs may find that 'traditional' incident handling procedures are not fit-for-purpose due to the challenges posed by the nature of cloud infrastructure such as scope of user control, multi-location and multi-tenancy (Duncan, Creese & Goldsmith 2015; Juliadotter & Choo 2015; Li, Li & Liu

2015; Yang et al. 2015). For example, a security incident of the hacking of Sony's network in 2011 was attributed to a hacker who rented the Amazon EC2 service (Ouedraogo & Mouratidis 2013). Another high profile incident is the iCloud data breach that resulted in the dissemination of nude photos and videos of popular celebrities (Apple Press Info 2014). The incident has generally affected the reputation of the cloud service provider even though Apple's investigation revealed that the breach was not a result of their system flaws.

Furthermore, the requirements and challenges of the incident handling principles faced by CSUs and CSPs are likely to differ, for example in terms of how and where to collect potential evidence and undertake post-incident investigation. Various studies have examined the challenges posed by cloud computing (Birk & Wegener 2011; Grobauer & Schreck 2010; Martini & Choo 2013; Monfared & Jaatun 2011a, 2011b; Quick & Choo 2013a, 2013b, 2013c, 2014; Ruan et al. 2011).When this research commenced in mid-2013, there were relatively few academic publications, suggesting that research in the area of cloud incident handling is somewhat elusive and still in its infancy.

1.3 Research aim and questions

The aim of this research is to design, develop, and validate an evidence-based cloud incident handling framework. This study consists of one overarching research question and three sub-research questions. The main research question is: How should security incidents for organisational cloud users is handled effectively?

The following sub-questions must be answered in order to address the above main question.

a) What are the impacts of cloud computing infrastructure on incident handling strategies (including post-incident investigations)?
b) Are changes to existing incident handling strategies required to better support organisational cloud users, and if so, what changes are required?
c) How can the proposed cloud incident handling framework be validated?

1.4 Research scope

The focus of this research was narrowed to the development and validation of the cloud incident handling framework. The framework is generally involves phases such as preparation, detection and analysis, incident response and post incident, which will be further discussed in Chapter 4. Technical experiments were conducted in a controlled environment such as virtual machine and mobile platform for framework validation.

1.5 Structure of the thesis

This thesis is organised into eight chapters. The following provides an overview of the structure.

Chapter 2 introduces information security incident handling, and discusses the role of digital forensics in incident handling, current research trends, and challenges posed by cloud computing to the landscape of incident handling. Subsequently, a high-level conceptual cloud incident handling framework is proposed.

Material presented in this chapter has appeared in the following publication:

- Ab Rahman, NH & Choo, K-KR 2015, 'A Survey of Information Security Incident Handling in the Cloud', *Computers & Security*, vol. 49, pp. 45–69.

Chapter 3 presents a study in two parts, undertaken to obtain viewpoints from industry practitioners. The first part was conducted to identify the challenges of emerging threats to incident handling and digital forensics by utilising Routine Activity Theory. In the second part, a conceptual model that draws upon the Situational Awareness Model and the Protection Motivation Theory was applied to identify the factors influencing the adoption of incident handling in the cloud.

Material presented in this chapter has appeared in the following publications:

- Ab Rahman, NH & Choo, K-KR 2015, 'Factors influencing the adoption of cloud incident handling strategy : A preliminary study in Malaysia', in *Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015).*
- Ab Rahman, NH, Kessler, G, and Choo, K-KR 2016. 'Implications of emerging technologies to incident handling and digital forensic strategies: A routine

activity theory', in K-KR Choo & A Dehghantanha (eds), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Syngress, an Imprint of Elsevier [In press].

Chapter 4 demonstrates the feasibility of the framework using an ownCloud (open source private Storage as a Service (StaaS) solution) case study simulation. It also explains how the Situational Crime Prevention Theory can be used in the framework to design mitigation strategies.

Material presented in this chapter has appeared in the following publication:

- Ab Rahman, NH & Choo, K-KR 2015, 'Integrating Digital Forensic Practices in Cloud Incident Handling: A Conceptual Cloud Incident Handling Model', in R Ko & K-KR Choo (eds), *Cloud Security Ecosystem*, Syngress, an Imprint of Elsevier, Waltham, MA, pp. 383–400.

Chapter 5 validates the framework using mobile cloud storage as a case study. Three popular cloud storage applications were deployed, namely Dropbox, Google Drive, and OneDrive. The utility of the framework was demonstrated for organisational cloud users to undertake incident investigations (e.g. collect and analyse residual data from cloud storage applications).

Material presented in this chapter has appeared in the following publication:

- Ab Rahman, NH, Cahyani, NDW & Choo, KKR 2016, 'Cloud incident handling and forensic-by-design: cloud storage as a case study', *Concurrency and Computation: Practice and Experience*. DOI: http://dx.doi.org/10.1002/cpe.3868

Chapter 6 presents further validation of the framework using mobile communication applications as a case study. Five applications were deployed, namely WhatsApp, Telegram, Skype, Messenger and Viber. A scenario of the possible use of smart mobile technology in terrorism activities was considered. Common user activities were simulated to examine the potential evidence artefacts and their association with incident handling practices.

Material presented in this chapter has appeared in the following publications:

- Cahyani, NDW, Ab Rahman, NH, Xu, Z, Glisson, WB and Choo, K-K R 2016, 'The role of mobile forensics in terrorism investigations involving the use of cloud apps', in *Proceedings of the 9th International Conference on Mobile Multimedia Communications (MOBIMEDIA 2016)*,[In press].
- Cahyani, NDW, Ab Rahman, NH, Glisson, WB and Choo, K-K R 2016, 'The role of mobile forensics in terrorism investigations involving the use of cloud apps and communication apps', *Journal of Mobile Networks and Applications*, [In press].

Chapter 7 explores the importance of forensic-by-design (FBD) principles into a system or architecture. The concept of FBD is proposed as future work to ensure more proactive incident handling activities. Cyber-Physical Cloud System (CPCS) infrastructure is used as a discussion to illustrate the concept.

Material presented in this chapter has appeared in the following publication:

- Ab Rahman, NH, Glisson, WB, Yang, Y & Choo, K-KR 2016, 'Forensic-by-Design Framework for Cyber-Physical Cloud Systems', *IEEE Cloud Computing*, vol. 3, no. 1, pp. 50–59.

Chapter 8 presents the key findings and implications of this research, and highlights the scope for future research.

The thesis also includes a number of appendices that contain additional information in support of the main discussion, including a sample questionnaire and a sample of SQLite database acquisition results.

2 Information security incident handling: An overview

This chapter presents an insight into incident handling in the domain of information security and cloud computing, commencing by establishing definitions of incident management, incident handling, and incident response. It continues by discussing the common phases in incident handling and the role of digital forensics in incident handling. The next part discusses research trends based on the located materials, and follows with challenges posed by cloud computing to the landscape of incident handling. Subsequently, a high-level conceptual cloud incident handling framework is proposed.

Material presented in this chapter has appeared in the following publication:

- Ab Rahman, NH & Choo, K-KR 2015, 'A Survey of Information Security Incident Handling in the Cloud', *Computers & Security*, vol. 49, pp. 45–69.

2.1 Incident handling: A survey

Information security management is relatively mature, as evidenced by the number of international standards and guidelines, as well as the academic literature on the topic. Despite the maturity of this area, there is a lack of consistency in describing incident management, incident handling, and incident response in the literature. This section presents the distinctions between these terminologies, as explained in the remainder of this section (see Figure 1).

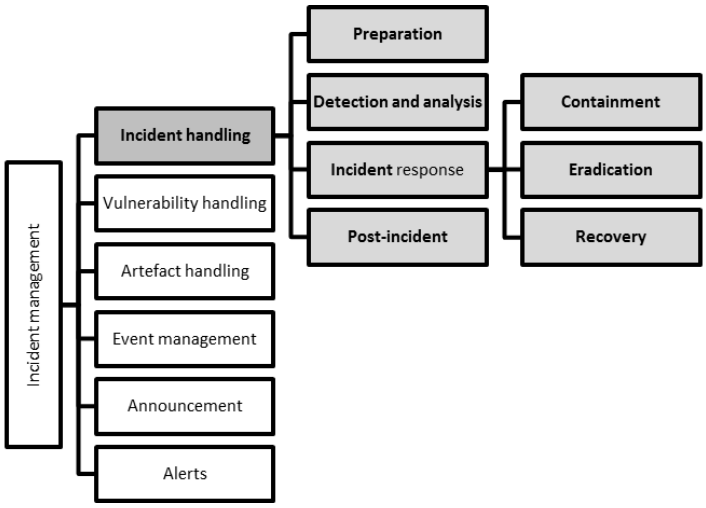

Figure 1 What is incident management? (Adapted from: Alberts et al. 2004; British Standards Institution 2007; Cichonski et al. 2012)

As explained by Alberts et al. (2004), incident management is not only about responding to an incident; it also includes vulnerability handling, artefact handling, security awareness training, and other related services.

Incident handling consists of incident reporting, incident analysis, and incident response (Killcrece 2003). Incident response refers to the collective actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to prevent future similar incidents. Similarly, the National Institute of Standards and Technology (NIST) (Cichonski et al. 2012) defines incident handling as the whole lifecycle that includes incident response. The latter relates to the ability to react to a security incident.

Grobauer and Schreck (2010) further explain that response should incorporate containment, eradication, and recovery phases, which is consistent with the proposed guidelines for Computer Security Incident Response Teams (CSIRT) (Alberts et al. 2004) and NIST (Cichonski et al. 2012). This is the definition adopted in this chapter, namely incident management is the ‘big picture’ (as presented in Figure 1) that comprises incident handling and incident response. The grey boxes in the Figure 1 represent the scope of this study.

2.1.1 Standards and guidelines

This section briefly describes several key international standards and guidelines, and our reviews of existing academic incident handling models.

Computer Emergency Response Team Coordination Centre (CERT/CC): CERT/CC, part of the Software Engineering Institute (SEI), located in Carnegie Mellon University (CMU), published a series of four guidelines for managing information security incidents. The Handbook for Computer Security Incident Response Teams (CSIRT) (West-Brown et al. 2003) is the main publication designed to provide specific in-depth guidance to support organisations in forming and operating a CSIRT (West-Brown et al. 2003). The State of the Practice for CSIRTs (Killcrece 2003) is designed to assist new and existing teams in understanding best practices and recommendations for handling incidents and related CSIRT services. The Organisational Models for CSIRT publication (Killcrece et al. 2003) focuses on selecting the right model for an organisation's incident response capabilities. Defining incident management processes for CSIRTs: A work in progress (Alberts et al. 2004) provides an overview of the processes and functions, and supporting people, technology, and procedures that are involved in incident management.

CERT/CC discusses four phases of the incident handling process model (i.e. receiving an incident report, triage, incident response, and analysing), which consists of 14 sub-phases.

NIST Special Publication (NIST SP 800-61): NIST is a non-regulatory federal agency within the US Department of Commerce. The Computer Security Division of NIST publishes Special Publications in the 800 series for the computer security community. SP 800-61 (Cichonski et al. 2012) is one of the 800 series documents that discusses computer security handling guidelines.

This guideline outlines four incident handling phases, namely (1) preparation, (2) detection and analysis, (3) containment, eradication, and recovery, and (4) post-incident activity. In NIST's incident handling model, the second (i.e. detection and analysis) and third (i.e. containment, eradication, and recovery) phases are illustrated as iterative, whereas the final phase is interconnected to the first phase.

This guideline includes a detailed description of each phase, and highlights some key points, such as recommendations for conducting incident analysis, incident documentation, and the sharing of information between team members and external parties.

International Organization for Standardization (ISO): ISO/IEC 27035:2011, an ISO information security incident management standard, is designed for large and medium-sized organisations (ISO 2011). The standard is not limited to incident handling, and covers processes for managing information security events and vulnerabilities.

Five phases are incorporated in the standard, namely (1) planning and preparation, (2) detection and reporting, (3) assessment and decision-making, (4) responses, and (5) lessons learnt. The phases are depicted as a lifecycle, as each phase is connected to the following phase, including the final phase being linked to the first phase.

This standard also provides a collection of reporting form templates for information security events, incidents, and vulnerabilities.

European Network and Information Security Agency (ENISA): ENISA is an agency of the European Union (EU) that was established to improve network and information security in the EU. As an agency of expertise, ENISA is actively contributing to specific technical and scientific tasks.

The Incident Management Guide is one ENISA publication that provides practical information and guidelines for the management of incident handling phases (ENISA 2010). The phases consist of six major sequence components, these being (1) incident report, (2) report registration, (3) triage, (4) incident resolution, (5) incident closure, and (6) post-analysis. ENISA's approach closely follows the CERT/CC approach, except for the inclusion of incident closure and post-analysis as the final phase. The guideline also incorporates a formal framework for a Computer Emergency Response Team (CERT), such as roles, workflows, and basic CERT policies.

SANS Institute: The SANS Institute is a well-known private US company that specialises in Internet Security training. In addition, the SANS research archive is publicly available, and is referred to as the SANS Reading Room. Many publications in various computer security areas can be accessed from the Reading Room, including those on incident handling matters.

The SANS Incident Handler's Handbook (Kral 2011) provides information for IT professionals and managers to create incident response policies, standards, and teams for their organisations. It incorporates six phases as follows, (1) preparation, (2) identification, (3) containment, (4) eradication, (5) recovery, and (6) lessons learnt. This handbook is quite brief compared to the other five guidelines discussed in this section. Its contents include a checklist for the incident handler, and guidelines on anomaly searching for Windows and UNIX operating systems.

Information Technology Infrastructure Library (ITIL): ITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the organisation. The ITIL publication consists of five volumes, and each one covers an ITSM lifecycle stage.

BIP 0107:2008—Foundations of IT Service Management Based on ITIL V3 (British Standards Institution 2007)—is a model for IT service management. Incident management is one of the service management areas. It consists of five main phases, (1) incident detection and recording, (2) classification and initial input, (3) investigation and diagnosis, (4) resolution and recovery, and (5) incident disclosure. These five phases are described as a process workflow. Event management is another service area that is closely related to incident management. It is concerned with monitoring events and detecting any triggered events for the incident management process.

2.1.2 Related works

A number of academic models or frameworks (both terms are used interchangeably) have been proposed by various authors, who discuss key phases and activities involved in the incident handling model.

Mitropoulos et al. (2006) proposed a framework that draws upon principles of digital forensics and incident handling and responses. It comprises six phases, namely (1) preparation, (2) identification, (3) containment, (4) eradication, (5) recovery and (6) follow-up. These phases are in line with the existing standards and recommendations, such as SANS (Kral 2011) and NIST (Cichonski et al. 2012). Another more recent study (Line 2013), based on the existing ISO/IEC 27035:2011 standard, presented a qualitative analysis that investigated current practices concerning information security incident management in the power industry.

Focusing on small-scale organisations and CSIRT, Kim et al. (2011) proposed a systematic approach for comprehensive incident handling that focused on bot response, covering detection, analysis, and response phases. The authors noted that the other phases of incident handling (i.e. preparation and post-incident) will be expanded on by large CSIRTs. The model of Khurana et al. (2009) uses a collaborative incident response and investigation mitigation strategy for multiple sites, which comprises four parallel phases at two sites (i.e. local and collaborative centre sites). The phase starts with incident preparation at both sites. It is followed by incident detection and strategy development at the local site, and in the meantime the collaborative centre starts using incident analysis once it has received an incident detection report. Both sites then conduct their investigations independently and finally close the incident collaboratively.

The emergence of cloud computing in recent years has led to several researchers examining incident handling in the cloud. For example, Grobauer and Schreck (2010) analysed the challenges and approaches that would be suitable for incident handling and response in the cloud. The challenges and approaches are examined for the following five common steps: (1) detection, (2) analysis, (3) containment, (4) eradication and recovery, and (5) preparation/continuous improvement.

Using an OpenStack environment (Infrastructure as a Service—IaaS) as a case study, Monfared and Jaatun (2012) demonstrated that the NIST incident handling guideline can be adapted for deployment in the cloud computing environment by introducing cloud specific strategies in each of the five phases.

The five key cloud strategies are specific cloud incident handling approaches, responsible stakeholder(s) for the approaches, service impacted, enforcement challenges, and specific platform and library dependencies.

A comparative summary of the six standards and guidelines, and the existing academic incident handling model is presented in Tables 1 and 2 respectively. As outlined in Table 1, the standards and guidelines of CERT/CC, BIP 0107:2008 and ENISA are reactive (i.e. services are triggered by an event or request). Both CERT/CC and ENISA incorporate incident preparation as part of the incident management framework, whereas BIP 0107:2008 discusses the issue with reference to event management (other sub-areas). This is consistent with several other published works (Anuar et al. 2011; Yuill et al. 2000), which pointed out that incident handling is primarily reactive. On the

References

Abadi, M, Abelson, H, Acquisti, A, Barak, B, Bellare, M, Bellovin, S, Blaze, M, Camp, L, Canetti, R, Cranor, LF, Dwork, C, Feigenbaum, J, Felten, E, Ferguson, N, Fischer, M, Ford, B, Franklin, M, Garay, J, Green, M, Halevi, S, Jha, S, Juels, A, Kaashoek, M, Krawczyk, H, Landau, S, Lee, W, Lysyanskaya, A, Malkin, T, Mazieres, D, McCurley, K, McDaniel, P, Micciancio, D, Myers, A, Pass, R, Paxson, V, Peha, J, Ristenpart, T, Rivest, R, Rogaway, P, Rose, G, Sahai, A, Schneier, B, Shacham, H, Shelat, A, Shrimpton, T, Silberschatz, A, Smith, A, Song, D, Tsudik, G, Vadhan, S, Wright, R, Yung, M & Zeldovich, N 2014, *Open letter from US researchers in cryptography and information security*, viewed 18 June 2014, <http://masssurveillance.info>.

Abdi, H 2003, 'Factor rotations in factor analyses', in M Lewis-Back, A Bryman, & T Futing (eds), *Encyclopedia of Social Sciences Research Methods*, Thousand-Oaks (Sage), California.

ACCA 2014, *Cloud Readiness Index 2014 - Executive Summary*, Asia Cloud Computing Association, viewed 16 February 2014, <http://asiacloudcomputing.org/research/cri2014>.

Afzaal, M, Di Sarno, C, Coppolino, L, DAntonio, S & Romano, L 2012, 'A resilient architecture for forensic storage of events in critical infrastructures', in *Proceedings of the 14th IEEE International Symposium on High-Assurance Systems Engineering*, pp. 48–55.

Agarwal, A, Gupta, M, Gupta, S & Gupta, SC 2011, 'Systematic digital forensic investigation model', *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 1, pp. 118–167.

Ahmad, A, Hadgkiss, J & Ruighaver, AB 2012, 'Incident response teams – challenges in supporting the organisational security function', *Computers & Security*, vol. 31, no. 5, pp. 643–652.

Ahmad, AR & Hamasaeed, NH 2014, 'The role of social media in the Syrian Civil War', in *Proceedings of the 3rd Conference on Communication, Media, Technology and Design*, pp. 284–289.

Alazab, M, Venkatraman, S & Watters, P 2009, 'Effective digital forensic analysis of the NTFS disk image', *Ubiquitous Computing and Communication Journal*, vol. 4, no. 3, pp. 551–558.

Albakri, SH, Shanmugam, B, Samy, GN, Idris, NB & Ahmed, A 2014, 'Security risk assessment framework for cloud computing environments', *Security and Communication Networks*, vol. 7, no. 11, pp. 2114–2124.

Alberts, C, Dorofee, A, Killcrece, G, Ruefle, R & Zajicek, M 2004, *Defining incident management processes for CSIRTs: A work in progress*, viewed 30 November 2013, <https://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14405.pdf>.

Aleem, A & Sprott, CR 2013, 'Let me in the cloud: analysis of the benefit and risk assessment of cloud platform', *Journal of Financial Crime*, vol. 20, no. 1, pp. 6–24.

Allan, D, Hahn, T, Whitmore, J & Buecker, A 2010, *Security in development : the IBM secure engineering framework*, IBM Redbooks, viewed 6 May 2015, <http://www.redbooks.ibm.com/abstracts/redp4641.html>.

Almulla, S, Iraqi, Y & Jones, A 2013, 'Cloud forensics: A research perspective', in *Proceeding of the 9th International Conference on Innovations in Information Technology (IIT)*, pp. 66–71.

Amazon Web Services 2014a, *Amazon CloudWatch*, viewed 28 October 2014, <http://aws.amazon.com/cloudwatch/>.

— 2014b, *Penetration testing*, viewed 3 May 2014, <https://aws.amazon.com/security/penetration-testing/>.

— 2014c, *Vulnerability reporting*, viewed 3 May 2014, <https://aws.amazon.com/security/vulnerability-reporting/>.

— 2016, *AWS shared responsibility model*, viewed 8 February 2016, <https://aws.amazon.com/compliance/shared-responsibility-model/>.

Amble, JC 2012, 'Combating terrorism in the new media environment', *Studies in Conflict & Terrorism*, vol. 35, no. 5, pp. 339–353.

Antonio, P & Labuschangne, L 2012, 'A conceptual model for digital forensic readiness', in *Proceedings of the 11th Information Security for South Africa (ISSA)*, pp. 1–8.

Anuar, NB, Furnell, S, Papadaki, M & Clarke, N 2011, 'A risk index model for security incident prioritisation', in *Proceedings of the 9th Australian Information Security Management Conference*, pp. 24–39.

Anuar, NB, Papadaki, M, Furnell, S & Clarke, N 2010, 'An investigation and survey of response options for Intrusion Response Systems (IRSs)', in *Proceedings of the 9th Information Security for South Africa (ISSA)*, pp. 1–8.

— 2012, 'A response strategy model for intrusion response systems', in D Gritzalis, S Furnell & M Theoharidou (eds), *Information Security and Privacy Research*, Springer Berlin Heidelberg, pp. 573–578.

— 2013, 'A response selection model for intrusion response systems : Response Strategy Model (RSM)', *Security and Communication Networks*, vol. 7, no. 11, pp. 1831–1848.

Anwar, T & Abulaish, M 2014, 'A social graph based text mining framework for chat log investigation', *Digital Investigation*, vol. 11, no. 4, pp. 349–362.

Apple Press Info 2014, *Update to Celebrity Photo Investigation*, viewed 16 May 2015, <https://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html>.

Ardi, S & Shahmehri, N 2009, 'A post-mortem incident modeling method', in *Proceedings of the 4th International Conference on Availability, Reliability and Security*, pp. 1018–1023.

Ariely, GA 2014, 'Adaptive Responses to Cyberterrorism', in TM Chen, L Jarvis & S Macdonald (eds), *Cyberterrorism: Understanding, Assessment, and Response*, pp. 175–195.

Ariffin, A, Choo, KR & Slay, J 2013, 'Digital camcorder forensics', in *Proceedings of the 11th Australasian Information Security Conference*, pp. 39–47.

Ariffin, A, D'orazio, C, Choo, K-KR & Slay, J 2013, 'iOS forensics: How can we recover deleted image files with timestamp in a forensically sound manner?', in *Proceedings of the 8th International Conference on Availability, Reliability and Security*, pp. 375–382.

Ariffin, A, Slay, J & Choo, K 2013, 'Data recovery from proprietary-formatted CCTV hard disks', in G Peterson & S Shenoi (eds), *Advances in Digital Forensics IX*, Springer Berlin Heidelberg, pp. 213–223.

Azfar, A, Choo, K-KR & Liu, L 2016, 'An Android social app forensics adversary model', in *Proceedings of 49th Annual Hawaii International Conference on System Sciences (HICSS 2016)*.

BAE Systems Detica 2012, *botCloud - An emerging platform for cyber-attacks*, viewed 18 June 2014, <http://baesystemsdetica.blogspot.com.au/>.

Balduzzi, M, Zaddach, J, Balzarotti, D & Loureiro, S 2012, 'A security analysis of Amazon's Elastic Compute Cloud service', in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pp. 1427–1434.

Bandura, A 1977, 'Self-efficacy: Toward a unifying theory of behavioral change', *Psychological Review*, vol. 84, no. 2, pp. 191–215.

Bang, J, Lee, C, Lee, S & Lee, K 2013, 'Damaged backup data recovery method for Windows mobile', *The Journal of Supercomputing*, vol. 66, no. 2, pp. 875–887.

Barske, D, Stander, A & Jordaan, J 2010, 'A digital forensic readiness framework for South African SME's', in *Proceedings of the 9th Information Security for South Africa*, pp. 1–6.

Bashir, MN, Kesan, JP, Hayes, CM & Zielinski, R 2011, 'Privacy in the cloud : Going beyond the contractarian paradigm', in *Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies*, pp. 21–27.

Baskerville, R, Spagnoletti, P & Kim, J 2014, 'Incident-centered information security: Managing a strategic balance between prevention and response', *Information & Management*, vol. 51, no. 1, pp. 138–151.

Beebe, NL & Clark, JG 2005, 'A hierarchical, objectives-based framework for the digital investigations process', *Digital Investigation*, vol. 2, no. 2, pp. 147–167.

Bhilare, DS, Ramani, AK & Tanwani, S 2010, 'An architecture for a distributed collaborative inter university incident handling mechanism', *International Journal of Computer and Internet Security*, vol. 2, no. 1, pp. 29–39.

Bing, S, Hai-Feng, W & Ling, C 2012, 'Study of network security situation in honeynet', in *Proceedings of 2012 International Conference on Modelling, Identification and Control*, Shanghai, pp. 519–523.

Birk, D & Wegener, C 2011, 'Technical issues of forensic investigations in cloud computing environments', in *Proceedings of the 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–10.

Blank, R & Gallagher, P 2012, *NIST SP 800-30: Guide for Conducting Risk Assessments*, Gaithersburg, Tech. Rep.DOI: http://dx.doi.org/10.6028/NIST.SP.800-30r1

Böhme, R 2010, 'Security metrics and security investment models', in I Echizen, N Kunihiro & R Sasaki (eds), *Advances in Information and Computer Security*, Springer Berlin Heidelberg, pp. 10–24.

Bojanc, R 2013, 'A quantitative model for information-security risk management', *Engineering Management Journal*, vol. 25, no. 2, pp. 25–37.

Bojanc, R, Jerman-Blažič, B & Tekavčič, M 2012, 'Managing the investment in information security technology by use of a quantitative modeling', *Information Processing & Management*, vol. 48, no. 6, pp. 1031–1052.

British Standards Institution 2007, *BIP 0107:2008 Foundations Of It Service Management Based On Itil V3*, UK.

Brown TA 2006, *Confirmatory factor analysis for applied research*, The Guilford Press, New York and London.

Buyya, R, Vecchiola, C & Selvi, ST 2013, 'Cloud computing architecture', in *Mastering Cloud Computing:Technologies and Applications Programming*, Morgan Kaufmann, pp. 111–140.

Cahyani, NDW, Martini, B & Choo, K-KR 2015, 'Using multimedia presentations to improve digital forensic understanding: a pilot study', in *Proceedings of the 26th Australasian Conference on Information Systems (ACIS 2015)*, pp. 1–10.

Cárdenas, AA, Amin, S & Lin, Z 2011, 'Attacks against process control systems : Risk assessment, detection, and response', in *Proceedings of the 6th ACM symposium on information, computer and communications security*, pp. 355–366.

Caskurlu, B, Gehani, A, Bilgin, CC & Subramani, K 2013, 'Analytical models for risk-based intrusion response', *Computer Networks*, vol. 57, no. 10, pp. 2181–2192.

Cavusoglu, H, Mishra, B & Raghunathan, S 2004, 'A model for evaluating IT security investments', *Communications of the ACM*, vol. 47, no. 7, pp. 87–92.

Chabot, Y, Bertaux, A, Nicolle, C & Kechadi, M-T 2014, 'A complete formalized

knowledge representation model for advanced digital forensics timeline analysis', *Digital Investigation*, vol. 11, pp. 95–105.

Chivers, H, Clark, J a. & Cheng, P-C 2009, 'Risk profiles and distributed risk assessment', *Computers & Security*, vol. 28, no. 7, pp. 521–535.

Choo, KKR 2008, 'Organised crime groups in cyberspace: a typology', *Trends in Organized Crime*, vol. 11, no. 3, pp. 270–295.

Choo, K-KR 2010, *Cloud computing: challenges and future direction*, Trends & Issues in Crime and Criminal Justice, vol. 400, pp. 1–6, viewed 1 February 2014, <http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi400.pdf>.

— 2011, 'The cyber threat landscape: challenges and future research directions', *Computer & Security*, vol. 30, no. 8, pp. 719–731.

— 2014a, 'A conceptual interdisciplinary plug-and-play cyber security framework', in H Kaur & X Tao (eds), *ICTs and the Millennium Development Goals – A United Nations Perspective*, Springer, New York, USA, pp. 81–99.

— 2014b, 'Legal issues in the cloud', *IEEE Cloud Computing Magazine*, vol. 1, no. 1, pp. 94–96.

Choo, K-KR, Smith, RG, Walters, J & Bricknell, S 2013, *Perceptions of money laundering and financing of terrorism in the Australian legal profession*, *Research and Public Policy*, vol. 122, Canberra, no. 1.

Choo, KR, Smith, R & McCusker, R 2007, *Future directions in technology-enabled crime: 2007–09*, Research and Public Policy, no. 78, viewed 30 May 2013, <http://www.aic.gov.au/media_library/publications/rpp/78/rpp078.pdf>.

Chung, H, Park, J, Lee, S & Kang, C 2012, 'Digital forensic investigation of cloud storage services', *Digital Investigation*, vol. 9, no. 2, pp. 81–95.

Cichonski, P, Millar, T, Grance, T & Scarfone, K 2012, 'Computer security incident handling guide', *International Journal of Computer Research*, vol. 20, no. 4, pp. 459–530.

Citrix 2015, *Secure by design: how XenAPP dramatically simplifies data protection, access control and other critical security tasks*, viewed 20 May 2015, <https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/secure-by-design.pdf>.

Claar, CL & Johnson, J 2012, 'Analyzing home PC security adoption behavior', *Journal of Computer Information Systems*, vol. 52, no. 4, pp. 20–29.

Clarke, R V 1997, *Situational crime prevention: successful case studies*, 2nd edn, Harrow and Heston, New York.

Clarke, RA, Morell, MJ, Stone, GR, Sunstein, CR & Swire, P 2013, *Liberty and security in a changing world: Report and recommendations of the President's review group on intelligence and communications technologies*, Group on Intelligence and

Communication, Washington D.C., viewed 5 May 2014, <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

Cloud Security Alliance 2011, *Security guidance for critical areas of focus in cloud computing*, CSA, viewed 1 August 2014, <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>.

— 2013, *The notorious nine cloud computing top threats in 2013*, CSA, viewed 12 July 2013, <http://www.cloudsecurityalliance.org/topthreats/>.

— 2016, *The treacherous 12 - cloud computing top threats in 2016*, CSA, viewed 1 March 2016, <https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf>.

CMMI Product Team 2010, *CMMI® for Services, Version 1.3*, CMU/SEI, Pittsburgh.

Cohen, F 2009, 'Toward a science of digital forensic evidence examination', in *Advances in Digital Forensics VI*, Springer Berlin Heidelberg, pp. 17–35.

Cohen, LE & Felson, M 1979, 'Social change and crime rate trends: a Routine Activity approach', *American Sociological Review*, vol. 44, no. 4, pp. 588–608.

Connell, A, Palko, T & Yasar, H 2013, 'Cerebro: A platform for collaborative incident response and investigation', in *Proceedings of the 12th IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 241–245.

Connell, A & Waits, T 2013, 'The CERT assessment tool: Increasing a security incident responder's ability to assess risk', in *Proceedings of the 12th IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 236–240.

Cronbach, LJ & Meehl, P 1955, 'Construct validity in psychological', *Psychological Bulletin*, vol. 52, pp. 281-302.

Cusack, B & Kyaw, AK 2012, 'Forensic readiness for Wireless Medical Systems', in *Proceedings of the 10th Australian Digital Forensics Conference*, pp. 21–32.

Cusick, JJ & Ma, G 2010, 'Creating an ITIL inspired Incident Management approach: Roots, response, and results', in *Network Operations and Management Symposium Workshops (NOMS Wksps)*, pp. 142–148.

D'Orazio, C, Ariffin, A & Choo, KR 2014, 'iOS Anti Forensics: How can we securely conceal , delete and insert data?', in *Proceedings of the 47th Hawaii International Conference on System Sciences*, pp. 6–9.

Daley, R, Millar, T & Osorno, M 2011, 'Operationalizing the coordinated incident handling model', in *Proceedings of the 10th IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 287–294.

Danezis, G, Domingo-Ferrer, J, Hansen, M, Hoepman, J-H, Le Métayer, D, Tirtea, R & Schiffner, S 2014, *Privacy and Data Protection by Design – from policy to engineering*, ENISA, viewed 20 May 2015, <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-

design/at_download/fullReport>.

Dekker, M, Liveri, D & Lakka, M 2013, *Cloud security incident reporting framework for reporting about major cloud security incidents*, ENISA, Athens.

Denning, DE 2015, 'Toward more secure software', *Communications of the ACM*, vol. 58, no. 4, pp. 24–26.

DigitalCorpora 2015, *Govdocs1*, viewed 20 November 2015, <digitalcorpora.org/corp/files/govdocs1/>.

Ding, X & Zou, H 2011, 'Time based data forensic and cross-reference analysis', in *Proceedings of the 2011 ACM Symposium on Applied Computing*, pp. 185–190.

Dropbox 2014, *Dropbox for Business Security:*, Dropbox White Paper, viewed 25 November 2015, <https://www.dropbox.com/static/business/resources/dfb_security_whitepaper.pdf>.

Duncan, A, Creese, S & Goldsmith, M 2015, 'An overview of insider attacks in cloud computing', *Concurrency Computation: Practice and Experience*, vol. 27, no. 12, pp. 2964–2981.

Dykstra, J & Sherman, AT 2012, 'Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques', *Digital Investigation*, vol. 9, pp. 90–98.

— 2013, 'Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform', *Digital Investigation*, vol. 10, pp. S87–S95.

Elyas, M, Ahmad, A, Maynard, SB & Lonie, A 2015a, 'Digital forensic readiness: Expert perspectives on a theoretical framework', *Computers & Security*, vol. 52, pp. 70–89.

— 2015b, 'Digital forensic readiness: Expert perspectives on a theoretical framework', *Computers & Security*, vol. 52, pp. 70–89.

Elyas, M, Maynard, SB, Ahmad, A & Lonie, A 2014, 'Towards a systematic framework for digital forensic readiness', *Journal of Computer Information System*, vol. 54, no. 3, pp. 97–106.

Endsley, MR 1995, 'Toward a theory of situation awareness in dynamic systems', *Human Factors*, vol. 37, no. 1, pp. 32–64.

ENISA 2010, *Good practice guide for incident management*, ENISA, Athens.

— 2014, *ENISA threat landscape 2014: Overview of current and emerging cyber-threats*, ENISA Threat Landscape 2014, viewed 6 September 2015, <http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013>.

European Union Agency for Network and Information Security 2013, *Good practice guide for securely deploying governmental clouds*, Heraklion, Greece, pp. 1–46, viewed

12 August 2013, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds>.

Farhood, ND, Dehghantanha, A, Eterovic-Soric, B & Choo, K-KR 2015, 'Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms', *Australian Journal of Forensic Sciences*, pp. 1–20. DOI: http://dx.doi.org/10.1080/00450618.2015.1066854

Farina, J, Scanlon, M & Kechadi, M-T 2014, 'BitTorrent Sync: First impressions and digital forensic implications', *Digital Investigation*, vol. 11, pp. 77–86.

Federal Bureau of Investigation 2016, *Statement to Address Misleading Reports that the County Of San Bernardino Reset Terror Suspect's Iphone without Consent of the FBI*, viewed 30 January 2016, <https://assets.documentcloud.org/documents/2716811/Statement-from-the-FBI-Feb-20-2016.pdf>.

Fessi, BA, Benabdallah, S, Boudriga, N & Hamdi, M 2014, 'A multi-attribute decision model for intrusion response system', *Information Sciences*, vol. 270, pp. 237–254.

Freiling, FC & Schwittay, B 2007, 'A common process model for incident response and computer forensics', in *Proceedings of the 2007 IT Incident Management & IT Forensics (IMF 2007)*, pp. 19–40.

Frühwirth, C & Männistö, T 2009, 'Improving CVSS-based vulnerability prioritization and response with context information', in *Proceedings of the 3rd International Symposium on Empirical Software Enginnering and Measurement*, pp. 535–544.

Futcher, L & von Solms, R 2008, 'Guidelines for secure software development', in *Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries Riding the Wave of Technology - SAICSIT '08*, pp. 56–65.

Garfinkel, S, Nelson, AJ & Young, J 2012, 'A general strategy for differential forensic analysis', *Digital Investigation*, vol. 9, pp. 50–59.

Glisson, WB & Welland, R 2014, 'Web Engineering Security (WES) methodology', *Communications of the Association for Information Systems*, vol. 34, no. 1, pp. 1359–1396.

Google 2012, *Google's approach to IT security*, Google White Paper, viewed 25 November 2015, <https://static.googleusercontent.com/media/www.google.com/en/AU/work/pdf/whygoogle/google-common-security-whitepaper.pdf>.

Grispos, G, Glisson, WB, Pardue, JH & Dickson, M 2014, 'Identifying user behavior from residual data in cloud-based synchronized apps', *Journal of Information Systems Applied Research*, vol. 8, no. 2, pp. 4–14.

Grispos, G, Glisson, WB & Storer, T 2013a, 'Cloud security challenges: Investigating policies, standards and guidelines in a Fortune 500 organization', in *Proceeding of the 21st European Conference on Information Systems (ECIS)*, pp. 1–12.

— 2013b, ‘Using smartphones as a proxy for forensic evidence contained in cloud storage services’, in *Proceedings of the 46th Annual Hawaii International Conference on System Sciences*, pp. 4910–4919.

— 2015a, ‘Recovering residual forensic data from smartphone interactions with cloud storage providers’, in R Ko & K-KR Choo (eds), *Cloud Security Ecosystem*, Syngress, an Imprint of Elsevier, Waltham, MA, pp. 347–382.

— 2015b, ‘Security incident response criteria: A practitioner’s perspective’, in *Proceeding of the 21st Americas Conference on Information Systems (AMCIS)*.

Grobauer, B & Schreck, T 2010, ‘Towards incident handling in the cloud’, in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW ’10)*, pp. 77–85.

Grobler, CP, Louwrens, CP & von Solms, SH 2010, ‘A framework to guide the implementation of proactive digital forensics in organisations’, in *2010 International Conference on Availability, Reliability and Security*, pp. 677–682.

Grobler, M & Bryk, H 2010, ‘Common challenges faced during the establishment of a CSIRT’, in *Proceedings of the 9th Information Security for South Africa*, pp. 1–6.

Grover, J 2013, ‘Android forensics: Automated data collection and reporting from a mobile device’, *Digital Investigation*, vol. 10, pp. 12–20.

Guo, W & Wang, Y 2009, ‘An incident management model for SaaS application in the IT organization’, in *2009 International Conference on Research Challenges in Computer Science*, pp. 137–140.

Guo, Y, Slay, J & Beckett, J 2009, ‘Validation and verification of computer forensic software tools - searching function’, *Digital Investigation*, vol. 6, pp. 12–22.

Gurkok, C 2013, ‘Cyber Forensics and Incident Response’, in *Computer and Information Security Handbook*, 2nd edn, pp. 601–622.

Hadjidj, R, Debbabi, M, Lounis, H, Iqbal, F, Szporer, A & Benredjem, D 2009, ‘Towards an integrated e-mail forensic analysis framework’, *Digital Investigation*, vol. 5, no. 3-4, pp. 124–137.

He, W, Yuan, X, Yang, L & Science, C 2013, ‘Supporting case-based learning in information security with Web-based technology’, *Journal of Information Systems Education*, vol. 24, no. 1, pp. 31–41.

He, Y, Johnson, C, Renaud, K, Lu, Y & Jebrieli, S 2014, ‘An empirical study on the use of the Generic Security Template for structuring the lessons from information security incidents’, in *Proceedings of the 6th International Conference on CSIT*, pp. 178–188.

Herath, T & Rao, HR 2009, ‘Protection motivation and deterrence: A framework for security policy compliance in organisations’, *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125.

Herrmann, A, Morali, A, Etalle, S & Wieringa, R 2011, 'RiskREP : Risk-based security requirements elicitation and prioritization', in *Proceedings of the 1st International Workshop on Alignment of Business Process and Security Modelling*, pp. 1–8.

Hinduja, S & Kooi, B (2013), 'Curtailing cyber and information security vulnerabilities through situational crime prevention', *Security Journal*, vol. 26, no. 4, pp. 383–402.

Holt, TJ & Bossler, AM 2008, 'Examining the applicability of lifestyle-routine activities theory for cybercrime victimization', *Deviant Behavior*, vol. 30, no. 1, pp. 1–25.

Holt, TJ & Bossler, AM 2013, 'Examining the relationship between routine activities and malware infection indicators', *Journal of Contemporary Criminal*, vol. 29, no. 4, pp. 420–436.

Holtfreter, K, Reisig, MD & Pratt, TC 2008, 'Low self-control, routine activities, and fraud victimization', *Criminology*, vol. 46, no. 1, pp. 189–220.

Hooper, C, Martini, B & Choo, K-KR 2013, 'Cloud computing and its implications for cybercrime investigations in Australia', *Computer Law & Security Review*, vol. 29, no. 2, pp. 152–163.

Hove, C & Marte, T 2013, 'Information security incident management: An empirical study of current practice', Master's Thesis, Norwegian University of Science and Technology, Norway.

Hove, C, Marte, T, Line, MB & Bernsmed, K 2014, 'Information security incident management: Identified practice in large organizations', in *Proceedings of the 8th International Conference on IT Security Incident Management & IT Forensics*, pp. 27–46.

Hsu, CT, Luo, GH & Yuan, SM 2014, 'Personalized cloud storage system: A combination of LDAP distributed file system', in C-T Hsu, G-H Luo & S-M Yuan (eds), *Genetic and Evolutionary Computing*, Springer International Publishing, pp. 399–408.

Humaidi, N & Balakrishnan, V 2013, 'Exploratory Factor Analysis of user's compliance behaviour towards Health Information System's security', *Journal of Health & Medical Informatics*, vol. 4, no. 2, pp. 2–9.

Husain, MI & Sridhar, R 2010, 'iForensics : Forensic analysis of instant messaging on smart phones', in MI Husain & R Sridhar (eds), *Digital Forensics and Cyber Crime*, Springer Berlin Heidelberg, pp. 9–18.

Ifinedo, P 2012, 'Understanding information systems security policy compliance: An integration of the Theory of Planned Behavior and The Protection Motivation Theory', *Computers & Security*, vol. 31, no. 1, pp. 83–95.

Inglot, B & Liu, L 2014, 'Enhanced timeline analysis for digital forensic investigations', *Information Security Journal: A Global Perspective*, vol. 23, no. 1-2, pp. 32–44.

Irwin, D & Slay, J 2011, 'Extracting evidence related to VoIP calls', in G Peterson & S Shenoi (eds), *Advances in Digital Forensics VII*, Springer Berlin Heidelberg, pp. 221–228.

Ismail, S, Ahmad, A, Afizi, M & Shukran, M 2011, 'New method of forensic computing in a small organization', *Australia Journal Basic Application Science*, vol. 5, no. 9, pp. 2019–2025.

ISO 2011, *ISO/IEC 27035:2011 Information Technology - Security Techniques - Information Security Incident Management*, Geneva.

— 2013, *ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements*, Geneva.

— 2015, *ISO/IEC 27043:2015 - Information Technology -- Security Techniques -- Incident Investigation Principles and Processes*, Geneva.

Jansen, W & Grance, T 2011, *Guidelines on Security and Privacy in Public Cloud Computing*, Gaithersburg. DOI: http://dx.doi.org/10.6028/NIST.SP.800-144

Johnson, LR 2014, 'The stages of incident response', in *Computer Incident Response and Forensics Team Management*, pp. 21–35.

Johnston, BAC & Warkentin, M 2010, 'Fear appeals and information security behaviors: An empirical study', *Management Information System (MIS) Quarterly*, vol. 34, no. 3, pp. 549–566.

Juliadotter, NV & Choo, K-KR 2015, 'Cloud Attack and Risk Assessment Taxonomy', *IEEE Cloud Computing*, vol. 2, no. 1, pp. 14–20.

Jung, J, Jeong, C, Byun, K & Lee, S 2011, 'Sensitive privacy data acquisition in the iPhone for digital forensic analysis', in JJ Park, J Lopez, S-S Yeo, T Shon & D Taniar (eds), *Secure and Trust Computing, Data Management and Applications*, Springer Berlin Heidelberg, pp. 172–186.

Junqueira, FP, Reed, BC & Serafini, M 2011, 'Zab: High-performance broadcast for primary-backup systems', in *Proceedings of the 41st International Conference on Dependable Systems & Networks (DSN)*, pp. 245–256.

Kaart, M & Laraghy, S 2014, 'Android forensics: Interpretation of timestamps', *Digital Investigation*, vol. 11, no. 3, pp. 234–248.

Kácha, P 2009, 'Adapting the Ticket Request System to the needs of CSIRT teams', *WSEAS Transactions on Computers*, vol. 8, no. 9, pp. 1440–1450.

Karnouskos, S, Colombo, AW & Bangemann, T 2014, 'Trends and challenges for cloud-based industrial Cyber-Physical System', in AW Colombo, T Bangemann, S Karnouskos, J Delsing, P Stluka, R Harrison, F Jammes & JLM Lastra (eds), *Industrial Cloud-Based Cyber-Physical Systems*, Springer International Publishing, pp. 231–240.

Kearney, W & Kruger, H 2013, 'Effective Corporate Governance : Combining an ICT Security Incident and Organisational Learning', in *Proceedings of the 2nd International*

Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec 2013), pp. 12–21.

Kent, K, Chevaliar, S, Grance, T & Dang, H 2006, *Guide to integrating forensic techniques into incident response*, Gaithersburg, viewed 30 March 2014, <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>.

Kheir, N & Cuppens-boulahia, N 2010, 'A service dependency model for cost-sensitive intrusion response', in D Gritzalis, B Preneel & M Theoharidou (eds), *Computer Security–ESORICS 2010*, Springer Berlin Heidelberg, pp. 626–642.

Kheir, N, Debar, H, Boulahia, CN, Cuppens, F & Viinikka, J 2009, 'Cost evaluation for intrusion response using dependency graphs', in *Proceedings of the 1st IFIP International Conference on Network and Service Security*, pp. 1–6.

Khorshed, T, Ali, ABMS & Wasimi, SA 2012, 'A survey on gaps , threat remediation challenges and some thoughts for proactive attack detection in cloud computing', *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833–851.

Khurana, H, Basney, J, Bakht, M, Freemon, M, Welch, V & Butler, R 2009, 'Palantir : A framework for collaborative incident response and investigation', in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, pp. 38–51.

Khurana, H, Hadley, M, Lu, N & Frincke, DA 2010, 'Smart-grid security issues', *IEEE Security & Privacy*, vol. 1, no. Jan/Feb 2010, pp. 81–85.

Killcrece, G 2003, *State of the practice of Computer Security Incident Response Teams (CSIRTs)*, CMU/SEI, Pittsburgh.

Killcrece, G, Kossakowski, K-P, Ruefle, R & Zajicek, M 2003, *Organizational models for Computer Security Incident Response Teams (CSIRTs)*, CMU/SEI, Pittsburgh.

Kim, S-H, Choi, S-S, Park, H-S & Choi, J-W 2011, 'Advanced bot response mechanism based on DNS sinkhole', *Information International Interdisciplinary Journal*, vol. 14, no. 7, pp. 2499–2521.

Kissel, R, Stine, K, Scholl, M, Rossman, H, Fahlsing, J & Gulick, J 2008, *Security considerations in the System Development Life Cycle*. DOI: http://dx.doi.org/10.6028/NIST.SP.800-64r2

Klein, G, Rogge, H, Schneider, F, Toelle, J, Jahnke, M & Karsch, S 2010, 'Response initiation in distributed Intrusion Response Systems for tactical MANETs', in *Proceedings of the 2010 European Conference on Computer Network Defense*, pp. 55–62.

Kohn, MD, Eloff, MM & Eloff, JHP 2013, 'Integrated digital forensic process model', *Computers & Security*, vol. 38, no. 2013, pp. 103–115.

Koivunen, E 2012, '"Why wasn"t I notified?': Information security incident reporting demystified', in T Aura, K Jarvinen & K Nyberg (eds), *Information Security Technology for Application*, Springer Berlin Heidelberg, pp. 55–70.

Kostina, A, Miloslavskaya, N & Tolstoy, A 2009, 'Information security incident management process', in *Proceedings of the 2nd International Conference on Security of Information and Networks - SIN '09*, p. 93.

Kozlovszky, M, Kovacs, L, Torocsik, M, Windisch, G, Acs, S, Prem, D, Eigner, G, Sas, P, Schubert, T & Póserné, V 2013, 'Cloud security monitoring and vulnerability management', in *Proceedings of the 17th IEEE International Conference on Intelligent Engineering Systems*, no. 70, pp. 265–269.

Kral, P 2011, *Incident Handler's Handbook*, viewed 20 November 2013, <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.642.8488>.

Kulikova, O, Heil, R, van den Berg, J & Pieters, W 2012, 'Cyber crisis management: A Decision-Support framework for disclosing security incident information', in *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. 103–112.

Kundu, A & Ghosh, SK 2014, 'Game theoretic attack response framework for enterprise networks', in *Distributed Computing and Internet Technology*, Springer International Publishing, pp. 263–274.

Kurowski, S & Frings, S 2011, 'Computational documentation of IT incidents as support for forensic operations', in *Proceedings of the 6th International Conference on IT Security Incident Management and IT Forensics*, pp. 37–47.

Landman, M 2010, 'Managing smart phone security risks', in *Proceedings of the 2010 Conference on Information Security Curriculum Development (InfoSecCD)*, pp. 145–155.

Langner, R 2011, 'Dissecting a cyberwarfare weapon', *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51.

Computer Crimes Act 1997 (Malaysia).

Lee, J & Hong, D 2011, 'Pervasive forensic analysis based on mobile cloud computing', in *Proceedings of the 3rd International Conference on Multimedia Information Networking and Security*, pp. 572–576.

Lee, W, Fan, W, Miller, M, Stolfo, S & Zadok, E 2002, 'Toward cost-sensitive modeling for intrusion detection and response', *Journal of Computer Security*, vol. 10, no. 2, pp. 5–22.

Leom, M Di, Choo, K-KR & Hunt, R 2016, 'Remote wiping and secure deletion on mobile devices: A review', *Journal of Forensic Sciences*.[In press]

Li, B, Li, J & Liu, L 2015, 'CloudMon: A resource-efficient IaaS Cloud Monitoring System based on networked Intrusion Detection System virtual appliances', *Concurrency Computation Practice and Experience*, vol. 27, no. 8, pp. 1861–1885.

Li, H, Tian, X, Wei, W & Sun, C 2012, 'A deep understanding of cloud computing security issues in cloud computing', in H Li, X Tian, W Wei & C Sun (eds), *Network Computing and Information Security*, Springer Berlin Heidelberg, pp. 98–105.

Liang, H & Xue, Y 2010, 'Understanding security behaviors in personal computer usage: A Threat Avoidance perspective', *Journal of the Association for Information System*, vol. 11, no. 7, pp. 394–413.

Line, MB 2013, 'A Case Study: Preparing for the Smart Grids - Identifying current practice for information security incident management in the Power Industry', in *Proceedings of the 7th International Conference on IT Security Incident Management and IT Forensics*, pp. 26–32.

Line, MB & Moe, NB 2015, 'Understanding collaborative challenges in IT security preparedness exercises', in H Federrath & D Gollmann (eds), *ICT Systems Security and Privacy Protection*, Springer International Publishing, pp. 311–324.

Luo, Y, Szidarovszky, F, Al-nashif, Y & Hariri, S 2014, 'A fictitious play-based response strategy for multistage intrusion defense systems', *Security and Communication Networks*, vol. 7, no. 3, pp. 473–491.

Ma, WM 2010, 'Study on architecture-Oriented information security risk assessment model', in J-S Pan, S-M Chen & NT Nguyen (eds), *Computational Collective Intelligence: Technologies and Applications*, Springer Berlin Heidelberg, pp. 218–226.

Maddux, JE & Rogers, RW 1983, 'Protection Motivation and Self-Efficacy: A revised theory of fear appeals and attitude change', *Journal of Experimental Social Psychology*, vol. 19, no. 5, pp. 469–479.

Mailloux, LO, Grimaila, MR, Colombi, JM, Hodson, DD & Baumgartner, G 2014, 'System security engineering for information systems', in B Akhgar & HR Arabnia (eds), *Emerging Trends in ICT Security*, Elsevier Inc., pp. 3–24.

Makutsoane, MP & Leonard, A 2014, 'A conceptual framework to determine the digital forensic readiness of a cloud service provider', in *Proceedings of the 2014 PICMET: Infrastructure and Service Integration*, pp. 3313–3321.

Marinescu, DC 2013, 'Cloud infrastructure', in *Cloud Computing:Theory and Practice*, 1st edn, Elsevier Inc., pp. 67–98.

Martini, B & Choo, K-KR 2012, 'An integrated conceptual digital forensic framework for cloud computing', *Digital Investigation*, vol. 9, no. 2, pp. 71–80.

— 2013, 'Cloud storage forensics: ownCloud as a case study', *Digital Investigation*, vol. 10, no. 4, pp. 1–13.

Martini, B & Choo, KR 2014a, 'Distributed filesystem forensics: XtreemFS as a case study', *Digital Investigation*, vol. 11, no. 4, pp. 295–313.

— 2014b, 'Remote programmatic vCloud forensics: A six-step collection process and a proof of concept', in *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014)*, pp. 935–942.

Martini, B, Do, Q & Choo, K-KR 2015, 'Mobile cloud forensics: An analysis of seven popular Android apps', in R Ko & K-KR Choo (eds), *Cloud Security Ecosystem*,

Syngress, an Imprint of Elsevier, Waltham, MA, pp. 309–345.

— 2016, 'Digital forensics in the cloud era: The decline of passwords and the need for legal reform', *Trends & Issues in Crime and Criminal Justice*, vol. [In press].

McGraw, G 2004, 'Software security', *IEEE Security & Privacy*, vol. 2, no. 2, pp. 80–83.

McKemmish, R 1999, 'What is forensic computing?', *Trends & Issue in Crime and Criminal Justice*, Canberra, no. 118, pp. 1–6.

Mckemmish, R 2008, 'When is digital evidence forensically sound?', in I Ray & S Shenoi (eds), *Advances in Digital Forensics IV*, Springer US, pp. 3–15.

Mejri, MN, Ben-Othman, J & Hamdi, M 2014, 'Survey on VANET security challenges and possible cryptographic solutions', *Vehicular Communications*, vol. 1, no. 2, pp. 53–66.

Mell, P & Grance, T 2011, *The NIST Definition of Cloud Computing Recommendations*, National Institute of Standard and Technology, Gaithersburg.

Mellado, D, Blanco, C, Sánchez, LE & Fernández-Medina, E 2010, 'A systematic review of security requirements engineering', *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 153–165.

Meso, P, Ding, Y & Xu, S 2013, 'Applying Protection Motivation Theory to information security training for college student', *Journal of Information Privacy and Security*, vol. 9, no. 1, pp. 47–67.

Microsoft 2014a, *Microsoft Enterprise Cloud Red Teaming*, viewed 6 May 2015, <http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf.>.

— 2014b, *Security and Compliance: Office 365*, Microsoft White Paper, viewed 25 November 2015, <http://www.microsoft.com/en-us/download/confirmation.aspx?id=26552>.

Miller, J 2012, 'Individual offending, routine activities, and activity settings : revisiting the Routine Activity Theory of general deviance', *Journal of Research in Crime and Delinquency*, vol. 50, pp. 390–416.

Minárik, T & Osula, A-M 2016, 'Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law', *Computer Law & Security Review*, vol. 32, no. 1, pp. 111–127.

Mishra, S 2003, 'Exploitation of Information and Communication Technology by terrorist organisations', *Strategic Analysis*, vol. 27, no. 3, pp. 439–462.

Mitropoulos, S, Patsos, D & Douligeris, C 2006, 'On incident handling and response: A state-of-the-art approach', *Computers & Security*, vol. 25, no. 5, pp. 351–370.

Modi, C, Patel, D & Borisaniya, B 2013, 'A survey on security issues and solutions at

different layers of cloud computing', *The Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592.

Monfared, A & Jaatun, MG 2012, 'Handling compromised components in an IaaS cloud installation', *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 1, no. 1, pp. 1–21.

Monfared, AT & Jaatun, MG 2011a, 'As strong as the weakest link: Handling compromised components in OpenStack', in *Proceedings of the 3rd Third International Conference on Cloud Computing Technology and Science*, pp. 189–196.

— 2011b, 'Monitoring intrusions and security breaches in highly distributed cloud environments', in *Proceedings of the 3rd International Conference on Cloud Computing Technology and Science*, pp. 772–777.

Morrissey, S 2010, *iOS forensic analysis for iPhone, iPad, and iPod touch*, APress.

Moser, A & Cohen, MI 2013, 'Hunting in the enterprise: forensic triage and incident response', *Digital Investigation*, vol. 10, no. 2, pp. 89–98.

Mu, C & Li, Y 2010, 'An intrusion response decision-making model based on hierarchical task network planning', in *Expert Systems with Applications*, vol. 37, no. 3, pp. 2465–2472.

Mulazzani, M, Schrittwieser, S, Leithner, M, Huber, M & Weippl, E 2011, 'Dark clouds on the horizon : Using cloud storage as attack vector and online slack space', in *Proceedings of the 2011 USENIX Security Symposium*, pp. 65–76.

Multimedia Development Corporation 2012, *MSC Malaysia Cloud Initiatives*, viewed 16 February 2015, <http://www.mscmalaysia.my/cloud_computing>.

Murray, R & Ruefle, M 2014, *CSIRT requirements for situational awareness*, CMU/SEI, Pittsburgh, viewed 3 January 2015, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA596848>.

Al Mutawa, N, Baggili, I & Marrington, A 2012, 'Forensic analysis of social networking applications on mobile devices', *Digital Investigation*, vol. 9, no. 2012, pp. 24–33.

Mylonas, A, Meletiadis, V, Tsoumas, B & Mitrou, L 2012, 'Smartphone forensics : A proactive investigation scheme for evidence acquisition', in *Information Security and Privacy Research*, Springer Berlin Heidelberg, pp. 249–260.

National Institute of Standards and Technology (NIST) 2004, *Digital data acquisition tool specification*, viewed 3 January 2015, < http://www.cftt.nist.gov/Pub-Draft-1-DDA-Require.pdf >.

Nepal, S, Ranjan, R & Choo, K-KR 2015, 'Trustworthy processing of healthcare big data in hybrid clouds', *IEEE Cloud Computing*, vol. 2, no. 2, pp. 78–84.

Ng, B-Y, Kankanhalli, A & Xu, Y 2009, 'Studying users' computer security behavior:

A health belief perspective', *Decision Support Systems*, vol. 46, no. 4, pp. 815–825.

Ngobeni, S, Venter, H & Burke, I 2010, 'A forensic readiness model for wireless networks', in S Ngobeni, H Venter & I Burke (eds), *Advances in Digital Forensic VII*, Springer Berlin Heidelberg, pp. 107–117.

— 2012, 'The modelling of a digital forensic readiness approach for wireless Local Area Networks', *Journal of Universal Computer Science*, vol. 18, no. 12, pp. 1721–1740.

Nikkel, BJ 2014, 'Fostering incident response and digital forensics research', *Digital Investigation*, vol. 11, no. 4, pp. 249–251.

Nowruzi, M, Jazi, HH, Dehghan, M, Shahmoradi, M, Hashemi, SH & Babaeizadeh, M 2012, 'A comprehensive classification of incident handling information', in *Proceedings of the 6th International Symposium on Telecommunications (IST)*, pp. 1071–1075.

Ntantogian, C, Apostolopoulos, D, Marinakis, G & Xenakis, C 2014, 'Evaluating the privacy of Android mobile applications under forensic analysis', *Computers & Security*, vol. 42, pp. 66–76.

Nunally, J 1978, *Psychometric Theory*, McGraw-Hill, New York.

Ogun, MN 2012, 'Terrorist use of Internet: Possible suggestions to prevent the usage for terrorist purposes', *Journal of Applied Security Research*, vol. 7, no. 2, pp. 203–217.

Omeleze, S & Venter, HS 2013, 'Testing the harmonised digital forensic investigation process model-using an Android mobile phone', in *Proceedings of the 12th Information Security for South Africa (ISSA)*, pp. 1–8.

Ongaro, D, Rumble, SM, Stutsman, R, Ousterhout, J, Rosenblum, M, Organization, DOS & Distributed, D 2011, 'Fast crash recovery in RAMCloud', in *Proceedings of the 23rd ACM Symposium on Operating Systems Principles*, pp. 29–41.

Oriwoh, E, Jazani, D, Epiphaniou, G & Sant, P 2013, 'Internet of Things Forensics: Challenges and Approaches', in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 608–615.

Ou Yang, Y-P, Shieh, H-M & Tzeng, G-H 2013, 'A VIKOR technique based on DEMATEL and ANP for information security risk control assessment', *Information Sciences*, vol. 232, no. 2013, pp. 482–500.

Ouedraogo, M & Mouratidis, H 2013, 'Selecting a Cloud Service Provider in the age of cybercrime', *Computers & Security*, vol. 38, pp. 3–13.

Owen, P & Thomas, P 2011, 'An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines', *Digital Investigation*, vol. 8, no. 2, pp. 135–140.

Pangalos, G, Ilioudis, C & Pagkalos, I 2010, 'The importance of corporate forensic readiness in the information security framework', in *Proceedings of the 19th IEEE*

International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, pp. 12–16.

Pearson, S 2013, 'Privacy, security and trust in cloud computing', in S Pearson & G Yee (eds), *Privacy and Security for Cloud Computing*, Computer Communications and Networks, Springer London, London, pp. 3–42.

Pereira, MT 2009, 'Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records', *Digital Investigation*, vol. 5, no. 3-4, pp. 93–103.

Pilli, ES, Joshi, RC & Niyogi, R 2010, 'A generic framework for network forensics', *International Journal of Computer Applications*, vol. 1, no. 11, pp. 1–6.

Ping, L, Haifeng, Y & Guoqing, M 2010, 'An incident response decision support system based on CBR and ontology', in *Proceedings of the 2010 International Conference on Computer Application and System Modeling*, pp. 337–340.

Poolsappasit, N, Dewri, R & Ray, I 2012, 'Dynamic security risk management using Bayesian attack graphs', *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74.

Proctor, T 2013, 'The development of Warning , Advice and Reporting Points (WARPs) in UK national infrastructure', in S Bologna, B Hämmerli, D Gritzalis & S Wolthusen (eds), *Critical Information Infrastrucutre Security*, Springer Berlin Heidelberg, pp. 164–174.

Quick, D & Choo, K-KR 2013a, 'Digital droplets: Microsoft SkyDrive forensic data remnants', *Future Generation Computer Systems*, vol. 29, no. 6, pp. 1378–1394.

— 2013b, 'Dropbox analysis: data remnants on user machines', *Digital Investigation*, vol. 10, no. 1, pp. 3–18.

— 2013c, 'Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?', *Digital Investigation*, vol. 10, no. 3, pp. 266–277.

— 2014, 'Google Drive: Forensic analysis of cloud storage data remnant', *Journal of Network and Computer Applications*, vol. 40, no. 2014, pp. 179–193.

Quick, D, Martini, B & Choo, K-KR 2014, *Cloud storage forensics*, Syngress, an Imprint of Elsevier, Waltham, MA.

Rathfelder, C & Groenda, H 2015, 'LiveCloudInspector: Towards integrated IaaS forensics in the cloud', in A Bessani & S Bouchenak (eds), *Distributed Applications and Interoperable Systems*, vol. 9038, Springer International Publishing, pp. 207–220.

Reddy, K & Venter, H 2009, 'A forensic framework for handling information', in *Advances in Digital Forensics V*, Springer Berlin Heidelberg, pp. 143–155.

Reddy, K & Venter, HS 2013, 'The architecture of a digital forensic readiness management system', *Computers and Security*, vol. 32, pp. 73–89.

Reyns, BW 2013, 'Online routines and identity theft victimization: Further expanding

Routine Activity Theory beyond direct-contact offenses', *Journal of Research in Crime and Delinquency*, vol. 50, no. 2, pp. 216–238.

Rogers, RW 1975, 'A Protection Motivation Theory of fear appeals and attitude change', *The Journal of Psychology: Interdisciplinary and Applied*, vol. 91, no. 1, pp. 93–114.

Rong, C, Nguyen, ST & Jaatun, MG 2013, 'Beyond lightning: A survey on security challenges in cloud computing', *Computers & Electrical Engineering*, vol. 39, no. 1, pp. 47–54.

Rowlingson, R 2004, 'A ten step process for forensic readiness', *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1–28.

Ruan, K & Carthy, J 2013, 'Cloud computing reference architecture and its forensic implications : A preliminary analysis', in M Rogers & KC Seigfried-Spellar (eds), *Digital Forensics and Cyber Crime*, Springer Berlin Heidelberg, pp. 1–21.

Ruan, K, Carthy, J, Kechadi, T & Crosbie, M 2011, 'Cloud forensics', in G Peterson & S Shenoi (eds), *Advances in Digital Forensic VII*, Springer Berlin Heidelberg, pp. 35–46.

Ruefl, R, Dorofee, A, Mundie, D, Householder, AD, Murray, M & Perl, SJ 2014, 'Computer security incident response team development and evolution', *IEEE Security & Privacy*, vol. 12, no. 5, pp. 16–26.

Saha, A 2012, 'A look at ownCloud', *Linux Journal*, vol. 2012, no. 218, pp. 64–75.

Sarkar, SR, Mahindru, R, Hosn, RA, Vogl, N & Ramasamy, H V 2011, 'Automated incident management for a Platform-as-a-Service cloud', in *Proceedings of the 11th USENIX Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Network and Services*, pp. 5–11.

Satoh, N & Kumamoto, H 2009, 'Analysis of information security problem by probabilistic risk assessment', *International Journal of Computers*, vol. 3, no. 3, pp. 337–347.

Savada, AM, Metz, HC & Worden, RL 1999, *The sociology and psychology of terrorism: Who becomes a terrorist and why?*, viewed 25 March 2016, <https://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf>.

Shah, JJ & Malik, LG 2014, 'An approach towards digital forensic framework for cloud', in *2014 IEEE International Advance Computing Conference (IACC)*, pp. 798–801.

Shameli-Sendi, A, Cheriet, M & Hamou-Lhadj, A 2014, 'Taxonomy of intrusion risk assessment and response system', *Computers & Security*, vol. 45, pp. 1–16.

Shameli-Sendi, A & Dagenais, M 2013, 'ARITO: Cyber-attack response system using accurate risk impact tolerance', *International Journal of Information Security*, vol. 13, no. 4, pp. 367–390.

Shariatia, M, Dehghantanha, A & Choo, K-KR 2016, 'SugarSync forensic analysis', *Australian Journal of Forensic Sciences*, vol. 48, no. 1, pp. 95–117.

Shedden, P, Ahmad, A & Ruighaver, AB 2010, 'Organisational learning and incident response : Promoting effective learning through the incident response process', in *Proceedings of the 8th Australian Information Security Mangement Conference*, pp. 131–142.

— 2011, 'Informal learning in security incident response teams', in *Proceedings of 22nd Australasian Conference on Information Systems (ACIS 2011)*, p. Paper 37.

Shedden, P, Scheepers, R, Smith, W & Ahmad, A 2011, 'Incorporating a knowledge perspective into security risk assessments', *Vine: The Journal of Information and Knowledge Management Systems*, vol. 41, no. 2, pp. 152–166.

Shields, C, Frieder, O & Maloof, M 2011, 'A system for the proactive, continuous, and efficient collection of digital forensic evidence', *Digital Investigation*, vol. 8, no. 2011, pp. 3–13.

Shosha, AF, James, JI, Hannaway, A, Liu, C, Gladyshev, P & Shosha, A 2013, 'Towards automated malware behavioral analysis and profiling for digital forensic investigation purposes', in AF Shosha, JI James, A Hannaway, C-C Liu & P Gladyshev (eds), *Digital Forensics and Cyber Crime*, Springer Berlin Heidelberg, pp. 66–80.

Simon, M & Choo, K-KR 2014, 'Digital forensics: Challenges and future research directions', in I-S Kim & J Liu (eds), *Contemporary Trends in Asian Criminal Justice: Paving the Way for the Future*, Korean Institute of Criminology, Seoul, pp. 105–146.

Sindoori, R, Pallavi, P V & Abinaya, P 2012, 'An overview of disaster recovery in virtualization technology', *Journal of Artificial Intelligence*, vol. 6, no. 1, pp. 60–67.

Siponen, M, Adam Mahmood, M & Pahnila, S 2014, 'Employees' adherence to information security policies: An exploratory field study', *Information and Management*, vol. 51, no. 2, pp. 217–224.

Skopik, F, Ma, Z, Smith, P & Bleier, T 2012, 'Designing a cyber attack information system for national situational awareness', in N Aschenbruck, P Martini, M Meier & J Tölle (eds), *Future Security*, Springer Berlin Heidelberg, pp. 277–288.

Slay, J & Sitnikova, E 2009, 'The development of a generic framework for the forensic analysis of SCADA and process control systems', in M Sorell (ed.), *Forensics in Telecommunications, Information and Multimedia*, Springer Berlin Heidelberg, pp. 77–82.

Sonnenreich, W, Albanese, J & Stout, B 2006, 'Return on security investment (ROSI) – A practical quantitative model', *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 55–66.

Srinivasan, MK & Rodrigues, P 2012, 'State-of-the-art cloud computing security taxonomies: A classification of security challenges in the present cloud', in *Proceedings of the 2012 International Conference on Advances in Computing, Communications and Informatics*, pp. 470–476.

Stakhanova, N, Basu, S & Wong, J 2007, 'A taxonomy of intrusion response systems', *International Journal of Information and Computer Security*, vol. 1, no. 1/2, pp. 169–184.

Strasburg, C, Stakhanova, N, Basu, S & Wong, JS 2009a, 'A framework for cost sensitive assessment of intrusion response selection', in *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference*, pp. 355–360.

— 2009b, 'Intrusion response cost assessment methodology', in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09)*, pp. 388–391.

Subashini, S & Kavitha, V 2011, 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11.

Sylve, J, Case, A, Marziale, L & Richard, GG 2012, 'Acquisition and analysis of volatile memory from android devices', *Digital Investigation*, vol. 8, no. 3-4, pp. 175–184.

Symantec Corporation 2016, *2016 Internet security threat report*, vol. 21, Symantec Corporation, California.

Takabi, H, James, BJ & Gail, JA 2010, 'Security and privacy challenges in cloud computing environments', *IEEE Security & Privacy Magazine*, vol. 8, no. 6, pp. 24–31.

Tan, Y, Jiang, H, Feng, D, Tian, L & Yan, Z 2011, 'CABdedupe: A causality-based deduplication performance booster for cloud backup services', in *Proceedings of the 2011 IEEE International Parallel & Distributed Processing Symposium*, pp. 1266–1277.

Tassone, C, Martini, B, Choo, KR & Slay, J 2013, 'Mobile device forensics: a snapshot', *Trends & Issues in Crime and Criminal Justice*, vol. 460, pp. 1–7.

Taylor, LP 2013, 'Developing an incident response plan', in *FISMA Compliance Handbook*, 2nd edn, pp. 95–115.

Taylor, M, Haggerty, J, Gresty, D & Lamb, D 2011, 'Forensic investigation of cloud computing systems', *Network Security*, vol. 2011, no. 3, pp. 4–10.

Taylor, RM 1990, 'Situational Awareness Rating Technique (SART): The development of a tool for Aircrew Systems Design', *Situational Awareness in Aerospace Operations*, vol. 37, no. 1, pp. 65–84.

Telegram 2016, *Telegram FAQ*, viewed 28 May 2016, <Telegram FAQ>.

Tewksbury, R & Mustaine, EE 2000, 'Routine Activities And Vandalism: A Theoretical And Empirical Study', *Journal of Crime and Justice*, vol. 23, no. 1, pp. 81–110.

Theoharidou, M, Kotzanikolaou, P & Gritzalis, D 2011, 'Risk assessment methodology for interdependent critical infrastructures', *Int. J. Risk Assessment and Management*, vol. 15, no. 2/3, pp. 128–148.

Theoharidou, M, Mylonas, A & Gritzalis, D 2012, 'A risk assessment method for smartphones', in *Information Security and Privacy Research*, Springer Berlin Heidelberg, pp. 443–456.

Thethi, N & Keane, A 2014, 'Digital forensics investigations in the cloud', in *Proceedings of the 4th IEEE International Advance Computing Conference (IACC)*, pp. 1475–1480.

Thorpe, S, Grandison, T, Campbell, A, Williams, J, Burrell, K & Ray, I 2013, 'Towards a forensic-based service oriented architecture framework for auditing of cloud logs', in *Proceedings of the 9th World Congress on Services*, pp. 75–83.

Tøndel, IA, Line, MB & Jaatun, MG 2014, 'Information security incident management: Current practice as reported in the literature', *Computers & Security*, vol. 45, no. 2014, pp. 42–57.

Trček, D, Abie, H, Skomedal, A & Starc, I 2010, 'Advanced framework for digital forensic technologies and procedures', *Journal of Forensic Sciences*, vol. 55, no. 6, pp. 1471–80.

Trenwith, PM & Venter, HS 2013, 'Digital forensic readiness in the cloud', in *Proceedings of the 12th International Information Security South Africa (ISSA 2013)*, pp. 1–5.

Tsalis, N, Theoharidou, M & Gritzalis, D 2013, 'Return on security investment for cloud platforms', in *Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science*, pp. 132–137.

UNODC 2012, *The use of the Internet for terrorist purposes*, New York, viewed 20 March 2016, <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>.

US District Court for the District of Columbia 2013, *Morandum opinion: Civil Action No. 13-0851 (RJL)*, viewed 18 June 2014, <http://s3.documentcloud.org/documents/901810/klaymanvobama215.pdf>.

US GAO 2015, *Air traffic control: FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen*, viewed 20 November 2015, <www.gao.gov/products/GAO-15-370>.

Usmani, K, Mohapatra, AK & Prakash, N 2013, 'An improved framework for incident handling', *Information Security Journal: A Global Perspective*, vol. 22, no. 1, pp. 1–9.

Valiente, M-C, Garcia-Barriocanal, E & Sicilia, M-A 2012, 'Applying an ontology approach to IT service management for business-IT integration', *Knowledge-Based Systems*, vol. 28, pp. 76–87.

Valjarevic, A & Venter, H 2013, 'A harmonized process model for digital forensic investigation readiness', in G Peterson & S Shenoi (eds), *Advances in Digital Forensic IX, IFIP AICT*, Springer Berlin Heidelberg, pp. 67–82.

Valjarevic, A & Venter, HS 2011, 'Towards a digital forensic readiness framework for Public Key Infrastructure systems', in *Proceedings of the 10th International Information Security for South Africa (ISSA 2011)*, pp. 1–10.

Vance, A, Siponen, M & Pahnila, S 2012, 'Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory', *Information & Management*, vol. 49, no. 3, pp. 190–198.

Vidas, T, Zhang, C & Christin, N 2011, 'Toward a general collection methodology for Android devices', *Digital Investigation*, vol. 8, pp. 14–24.

Walters, J, Budd, C, Smith, RG, Choo, K-KR, Mccusker, R & Rees, D 2012, *Anti-oney laundering and counter-terrorism financing across the globe: A comparative study of regulatory action*, *Research and Public Policy*, vol. 113, Canberra.

Wang, J, Xiao, N & Rao, HR 2012, 'An exploration of risk information search via a search engine: Queries and clicks in healthcare and information security', *Decision Support Systems*, vol. 52, no. 2, pp. 395–405.

Webb, J, Ahmad, A, Maynard, SB & Shanks, G 2014, 'A situation awareness model for information security risk management', *Computers & Security*, vol. 44, pp. 1–15.

West-Brown, MJ, Stikvoort, D, Kossakowski, K-P, Killcrere, G, Ruefle, R & Zajicek, M 2003, *Handbook for computer security incident response teams (CSIRTs)*, 2nd edn, Carnegie Mellon/SEI, Pittsburgh.

Wiik, J, Davidsen, PI & Kossakowski, KP 2009a, 'Chronic workload problems in CSIRTs', in *Proceedings of the 27th International Conference of the System Dynamics Society*, pp. 1–19.

— 2009b, 'Persistent instabilities in the high-priority incident workload of CSIRTs', in *27th International Conference of the System Dynamics Society*, pp. 1–15.

— 2009c, 'Preserving a balanced CSIRT constituency', in *27th International Conference of the System Dynamics Society*, pp. 1–11.

Williams, ML 2015, 'Guardians upon high: An application of Routine Activities Theory to online identity theft in Europe at the country and individual level', *British Journal of Criminology*, vol. 56, no. 1, pp. 21–48.

Willison, R & Siponen, M, 2009, 'Overcoming the insider: reducing employee computer crime through Situational Crime Prevention', *Communications of the ACM*, vol. 52, no.9, pp.133-137.

Wood, T, Cecchet, E, Ramakrishnan, KK, Shenoy, P, Merwe, J Van Der & Venkataramani, A 2010, 'Disaster recovery as a cloud service : Economic benefits & beployment challenges University of Massachusetts Amherst', in *Proceedings of the 2nd USENIX Workshop on Hot Topics in Cloud Computing*, pp. 1–7.

Wu, T, Ferdinand, J, Disso, P, Jones, K, Campos, A & Pagna, J 2013, 'Towards a SCADA forensics architecture', in *Proceedings of the 1st International Symposium for ICS and SCADA Cyber Security Research*, pp. 12–21.

Wu, X, Fu, Y & Wang, J 2009, 'Information systems security risk assessment on improved fuzzy AHP', in *Proceedings of the 2nd ISECS International Colloquium on Computing, Communication, Control, and Management*, pp. 365–369.

Xia, R, Yin, X, Alonso, J, Machida, F & Trivedi, KS 2014, 'Performance and availability modeling of IT systems with data backup and restore', *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 4, pp. 375–389.

Xinlan, Z, Zhifang, H, Guangfu, W & Xin, Z 2010, 'Information security risk assessment methodology research: Group decision making and analytic hierarchy process', in *Proceedings of the 2nd World Congress on Software Engineering*, pp. 157–160.

Yang, J & Chen, Z 2010, 'Cloud computing research and security issues', in *Proceedings of the 2nd nternational Conference on Computational Intelligence and Software Engineering (CiSE)*, pp. 1–3.

Yang, TY, Dehghantanha, A, Choo, K-KR & Muda, Z 2016, 'Windows instant messaging app forensics: Facebook and Skype as case studies', *Plos One*, vol. 11, no. 3, pp. 1–29.

Yang, Y, Liu, JK, Liang, K, Choo, K-KR & Zhou, J 2015, 'Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data', in G Pernul, PYA Ryan & E Weippl (eds), *Computer Security -- ESORICS 2015*, Springer International Publishing, pp. 146–166.

Yegneswaran, V, Barford, P & Paxson, V 2005, 'Using honeynets for Internet situational awareness', in *Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets IV)*, pp. 17–22.

Yu, X, Jiang, L, Shu, H, Yin, Q & Liu, T 2009, 'A Process Model for Forensic Analysis of Symbian', in *Advances in Software Engineering*, Springer Berlin Heidelberg, pp. 86–93.

Yuill, J, Wu, F, Settle, J, Gong, F, Forno, R, Huang, M & Asbery, J 2000, 'Intrusion-detection for incident-response , using a military battlefiled-intelligence process', *Computer Networks*, vol. 34, no. 4, pp. 671–697.

Yunos, Z, Ahmad, R & Mohd Sabri, NA 2015, 'A qualitative analysis for evaluating a cyber terrorism framework in Malaysia', *Information Security Journal: A Global Perspective*, vol. 24, no. 1-3, pp. 15–23.

Zambon, E, Etalle, S, Wieringa, RJ & Hartel, P 2010, 'Model-based qualitative risk assessment for availability of IT infrastructures', *Software & Systems Modeling*, vol. 10, no. 4, pp. 553–580.

Zan, X, Gao, F, Han, J, Liu, X & Zhou, J 2010, 'NAIR: A novel automated intrusion response system based on decision making approach', in *Proceedings of the 5th IEEE International Conference on Information and Automation*, pp. 543–548.

Zeng, J, Feng, X, Wang, D & Fang, L 2014, 'Implemention of cyber security situation awareness based on knowledge discovery with trusted computer', in W Han, Z Huang,

C Hu, H Zhang & L Guo (eds), *Web Technologies and Applications*, Springer International Publishing, pp. 225–234.

Zhang, G, Yang, Y & Mao, X 2011, 'Disaster recovery evaluation PROC model framework based on information flow', in *Proceedings of the 1st International Conference on Computer Science and Network Technology (ICCSNT)*, pp. 1841–1845.

Zhang, L & Wang, W 2011, 'Constructions on disaster tolerant backup system of management information system', in *Proceedings of the 6th International Conference on Computer Science & Education (ICCSE)*, pp. 425–427.

Zhang, X, Liang, K & Zhang, X 2012, 'Research on the recovery strategy of incremental-data-based continuous data protection', in *Proceedings of the 14th International Conference on Computer Science and Electronics Engineering*, pp. 498–502.

Zhang, X, Wuwong, N, Li, H & Zhang, X 2010, 'Information security risk management framework for the cloud computing environments', in *Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, pp. 1328–1334.

Zhao, W & White, G 2014, 'Designing a formal model facilitating collaborative information sharing for community cyber security', in *Proceedings of the 47th Hawaii International Conference on System Sciences*, pp. 1987–1996.

Zhou, M & Yao, G 2012, 'Improved cost-sensitive model of intrusion response system based on clustering', in *Proceedings of the 2011 International Conference in Electrics, Communication and Automatic Control*, pp. 931–937.

Zielińska, E, Mazurczyk, W & Szczypiorski, K 2014, 'Trends in steganography', *Communications of the ACM*, vol. 57, no. 3, pp. 86–95.

Zimmerman, S & Glavach, D 2011, 'Cyber forensics in the cloud', *IAnewsletter*, vol. 14, no. 1, pp. 4–7.

Zissis, D & Lekkas, D 2012, 'Addressing cloud computing security issues', *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592.

Zonouz, S a., Khurana, H, Sanders, WH & Yardley, TM 2014, 'RRE: A game-theoretic intrusion response and recovery engine', *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 395–406.

Zonouz, S & Haghani, P 2013, 'Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior', *Computers & Security*, vol. 39, pp. 190–200.